



# Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 06 July 2005

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

## Daily Highlights

- Vnunet reports information technology experts have warned that, contrary to popular belief, two-factor authentication is not secure enough to curb Internet banking fraud. (See item [6](#))
- Agence France–Presse reports a global strategy to control the deadly bird flu virus within a decade was released by United Nations and animal health experts, who appealed for millions in donor funds to make the plan a reality. (See item [23](#))
- The Associated Press reports intelligence officials believe at least 50 terror groups now have some presence in Canada, where they are actively raising money and procuring weapons. (See item [32](#))

### DHS/IAIP Update Fast Jump

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS/IAIP Products & Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *July 05, Government Accountability Office* — GAO-05-421: Gasoline Markets: Special Gasoline Blends Reduce Emissions and Improve Air Quality, but Complicate Supply and Contribute to Higher Prices (Report). The Clean Air Act, as amended, requires some areas with especially poor air quality to use a “special gasoline blend” designed to reduce emissions of volatile organic compounds and nitrogen oxides and requiring the use of an oxygenate. In less severely polluted areas, the Act allows states, with Environmental Protection Agency

(EPA) approval, to require the use of other special blends as part of their effort to meet air quality standards. The Government Accountability Office (GAO) agreed to answer the following: (1) To what extent are special gasoline blends used in the United States and how, if at all, is this use expected to change in the future? (2) What effect has the use of these blends had on reducing vehicle emissions and improving overall air quality? (3) What is the effect of these blends on the gasoline supply? (4) How do these blends affect gasoline prices? GAO is making four recommendations to EPA, including that the agency, with the Department of Energy and others, develop a plan to balance the environmental benefits of using special fuels with the impacts of these fuels on the gasoline supply infrastructure.

Highlights: <http://www.gao.gov/highlights/d05421high.pdf>

Source: <http://www.gao.gov/new.items/d05669.pdf>

2. *July 05, Associated Press* — **United Nations nuclear agency may amend treaty to fight terrorism threat.** Delegates from about 100 countries began work Monday, July 4, to revamp an international treaty on protecting nuclear material, arguing existing laws fail to do enough to safeguard nuclear power plants from terrorism. The push to shield nuclear facilities has gained urgency since the attacks of September 11, 2001, amid new security concerns and nightmare scenarios of fuel-laden jumbo jets smashing into atomic power plants. "We can't go on with an old instrument in a new world," said the conference chairman, Alec Jean Baer of Switzerland. He said the proposed changes to the Convention on the Physical Protection of Nuclear Material would amount to an overhaul. The existing treaty was signed in Vienna and New York in 1980, long before the threat of terrorist nuclear attacks had become a pressing fear. It covers the international transport of nuclear material used for peaceful purposes, as well as some provisions on domestic storage and use. The changes under consideration by some 350 delegates would strengthen existing law by establishing an international standard to protect nuclear facilities from sabotage. The new changes also would call for cooperation between countries to locate and recover stolen and smuggled material and to combat such offenses. Convention on the Physical Protection of Nuclear Material:

[http://www.unodc.org/unodc/terrorism\\_convention\\_nuclear\\_material.html](http://www.unodc.org/unodc/terrorism_convention_nuclear_material.html)

Source: <http://www.gazettetimes.com/articles/2005/07/05/news/nation/tuenat09.txt>

3. *July 04, The Arizona Republic* — **New transformer to ensure adequate power supply.** Transformers needed to serve Phoenix's power delivery network have arrived from Canada and been installed at a north Phoenix substation. If tests go well, the Westwing substation could be running by Wednesday, July 6, utility officials from Arizona Public Service said. The use of Westwing, little-known before it erupted in flames last year and plunged the Phoenix area into a power crunch, would ensure a steady power supply as peak summer days arrive, effectively ending concern over electricity lingering from a year ago. A surge triggered by bird droppings led to a fire at the substation, destroying five transformers and severely limiting the amount of power that could be funneled into the Phoenix area. Area utilities issued a call to residents and businesses to conserve energy or face the prospect of rolling blackouts last summer. With Westwing back on the grid, the metro area's peak power supply will jump from 11,390 megawatts to 12,100 megawatts. That's well above what utilities forecast as the peak power demand, 10,860 megawatts. The prospect of thin power margins worried commissioners a week ago when temperatures surged past 110 degrees and power demand was forecast as high as 10,600 megawatts.

Source: <http://www.azcentral.com/12news/news/articles/0704westwing04-CP.html>

[\[Return to top\]](#)

## **Chemical Industry and Hazardous Materials Sector**

4. *July 02, Star-Ledger (NJ)* — **Elizabeth chemical fire injures four firefighters.** Four firemen suffered minor injuries battling a chemical fire at a warehouse in Elizabeth, NJ, on Friday morning, July 1, officials said. Two firemen were treated and released from Trinitas Hospital for heat exhaustion and inhalation from the fire at Advanced Foils Inc., 801 Magnolia Ave. Another firefighter was treated at the scene for lacerations, and another was taken to a local ambulatory care center with minor injuries, said Battalion Chief Thomas McNamara. No one was seriously injured in the blaze that started shortly after 10 a.m. (EDT) and lasted for about two hours, officials said. The cause of the fire was unknown, but toxic chemicals stored in the warehouse fueled the blaze until it became a three-alarm fire, said Fire Chief Edward Sisk. Authorities called for mutual aid from other departments, said Elizabeth Mayor J. Christian Bollwage, and contacted the state Department of Environmental Protection and the Union County Hazardous Materials Response Team. The chemicals that caught fire were toluene and xylene, commonly used in the production of Mylar foils found in products ranging from foil balloons to holographic wrapping paper.

Source: <http://www.nj.com/news/ledger/union/index.ssf?/base/news-0/112027997096370.xml&coll=1>

[\[Return to top\]](#)

## **Defense Industrial Base Sector**

Nothing to report.

[\[Return to top\]](#)

## **Banking and Finance Sector**

5. *July 05, InformationWeek* — **Banks will provide identity theft data to government.** Officials from the Identity Theft Assistance Center (ITAC) said on Tuesday, July 5, that they will provide information to the Federal Trade Commission (FTC) in order to aid law enforcement in catching perpetrators of identity theft crimes. The center is a bank-sponsored service that works with victims to restore their identities. Victims are referred to ITAC by their banks. ITAC walks victims through their credit reports, helps them place fraud alerts with credit bureaus, and notifies companies that appear to have had accounts opened fraudulently under victims' name. In its first year of operation, ITAC has helped 2,000 victims restore their identities. The FTC will place information collected from ITAC in its Consumer Sentinel database, which is accessible by more than 1,300 federal, state, and local law-enforcement agencies. The database is used as a source of information to further identity theft investigations, said George Handley, unit chief of the FBI's Financial Institution Fraud unit.

Identity Theft Assistance Center: <http://www.idtheftcenter.org/index.shtml>

Source: <http://www.informationweek.com/showArticle.jhtml;jsessionid=MSCIFWXDJQRESQSNDBCSKHSCJUMKJVN?articleID=165600565>

6. *July 04, Vnunet.com (UK)* — **Hackers crack two-factor security.** Information technology experts warned on Monday, July 4, that, contrary to popular belief, two-factor authentication is not secure enough to curb Internet banking fraud. "Two-factor is good, but hackers are responding," said Graham Cluley, senior technology consultant at anti-virus company Sophos. "The latest generation of spyware not only includes key-loggers that trap passwords, but screen-grabbing software. This takes multiple images of what the user is doing and sends it straight to the hacker," said Cluley. Cluley is not the only expert to warn of the danger of putting too much faith in two-factor technology, which combines conventional passwords with portable electronic tokens that generate a unique code in synchronization with a central security server. Bruce Schneier, chief technical officer at managed security services company Counterpane, has also raised doubts about the technology's ability to cope with man-in-the-middle and pharming attacks.

Source: <http://www.vnunet.com/vnunet/news/2139253/two-factor-authentication>

7. *July 04, Associated Press* — **Organization for Economic Cooperation and Development urges insurance for terror attack.** Some of the world's most advanced economies remain ill-equipped to survive the fallout from a major terrorist atrocity, the Organization for Economic Cooperation and Development (OECD) is warning, despite widespread efforts since the September 11 attacks to spread insurance risk between public and private sectors. "There are still significant gaps in coverage, which could be revealed by another large-scale attack," said OECD, a Paris-based organization of 30 industrialized countries, in a statement prepared for the release of their report on terrorism risk insurance. Almost four years after the terrorist attacks of September 11, the calculation of such risks remains fraught with difficulties and the worst kinds of attack are uninsurable, the study says. While governments are rightly devoting attention to preventing further attacks, the report adds, "ensuring financial coverage of the terrorism risk, if prevention were to fail, is a no less important policy issue to mitigate the potentially devastating impacts of future attacks." The report also cautions that insurance policies generally exclude the worst kind of scenario — such as when a chemical or nerve agent, nuclear device, or dirty bomb is used to attack a major city — and government guarantees often don't provide adequate cover.

Information on the OECD report:

[http://www.oecd.org/document/3/0,2340,en\\_2649\\_201185\\_3509299\\_5\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/3/0,2340,en_2649_201185_3509299_5_1_1_1_1,00.html)

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2005/07/04/AR2005070400803.html>

[[Return to top](#)]

## **Transportation and Border Security Sector**

8. *July 05, Associated Press* — **New Mexico airport facing serious growing pains.** Sightseeing motorists driving onto taxiways and near misses between aircraft and vehicles are just some of the growing pains at New Mexico's Santa Teresa Airport. The Dona Ana County airport's tenants say the situation is unsafe and criticize the county, which owns the airport, and airport manager Vernon Wilson, in particular, for not fixing the problems. At issue is public access for motorists to a taxiway, lack of fencing around the airport perimeter, and a number of other operational and management disputes. In one case, Joe Maxsom, a corporate pilot for Hunt

Building of El Paso, TX, who flies out of the airport, says he recently helped avoid a collision between a tractor-trailer being used in an airport construction project and a small Piper aircraft. He also said he sees motorists wander on to airport property to look at the planes several times a week. The airport has been growing lately. About 100 planes are based at the airport, nearly double the number of a decade ago, and a project is under way to lengthen the airport's runway to make it possible for DC-10s to land.

Source: [http://www.usatoday.com/travel/news/2005-07-05-nm-airport\\_x.htm](http://www.usatoday.com/travel/news/2005-07-05-nm-airport_x.htm)

9. *July 05, Department of Transportation* — **South Carolina State University receives grant for transportation education and research.** The U.S. Department of Transportation's Research and Innovative Technology Administration (RITA) announced on Tuesday, July 5, that just over \$1 million in grant money was awarded to South Carolina State University's James E. Clyburn University Transportation Center (UTC) to support the full range of the Center's education and research programs. A major component of the Center's work is its intermodal research, education, and technology transfer program, which recruits and trains minorities and women for the transportation workforce. More than 75 colleges and universities throughout the United States participate in the UTC program conducting transportation research, education, and technology transfer. The UTC program is administered by RITA, and grant recipients are required to provide matching funds.

More information on UTC grants can be found at <http://www.rita.dot.gov>

Source: <http://www.dot.gov/affairs/rita0605.htm>

10. *July 05, Department of Transportation* — **Research grant funds new technology to detect rail defects.** The Federal Railroad Administration (FRA) on Tuesday, July 5, announced the award of a safety research grant to the University of California at San Diego to develop new technology that helps detect rail defects. The university will receive a \$237,794 grant to research technology that will use ultrasonic waves and a pulsed laser to inspect the entire rail from top to bottom. Through this evaluation, the technology will be able to identify certain types of defects often missed by current inspection methods. Once the prototype is developed, the technology will be installed on FRA's newest track research vehicle, the T-18, which was recently added to the agency's fleet of automated track inspection vehicles. The agency's new National Rail Safety Action Plan calls for better rail inspection procedures as part of an aggressive effort to improve safety throughout the railroad industry. FRA also has studies underway to determine the effect of fatigue on different types of rail steels and how cracks develop and spread within rail; to review railroad crosstie construction design to ensure the rails stay in place and remain properly aligned; and to develop technologies to warn train crews of broken rails that lie ahead.

Source: <http://www.dot.gov/affairs/fra1605.htm>

11. *July 04, New York Times* — **With Congress's funding, a border fence may push to the sea.** Since 1997, the Border Patrol has been building a barrier wall extending 14 miles inland from the point along the coastline where Mexico and the United States meet. It started as a 10-foot-high wall made of military surplus steel landing mats used for aircraft in Vietnam. Over the years, the wall has been supplemented by a second fence made of steel mesh, with a lighted roadway between the two fences that is constantly monitored and patrolled by Border Patrol vehicles. But 3.5 miles of the project remain to be completed, with Smuggler's Gulch the most vulnerable spot along that span between the ocean and the San Ysidro border station, five



miles inland. Smuggler's Gulch is a 300-foot-deep gully that has been a prime route for bandits, border jumpers, and raw sewage from Tijuana to Southern California for more than 150 years. The U.S. Border Patrol wants to complete the last section, but has been stopped until now by environmental and regulatory roadblocks. This spring, as part a military spending bill, Congress gave the Border Patrol a green light to complete the fence.

Source: <http://www.nytimes.com/2005/07/04/national/04fence.html?8hpi&b&oref=login&oref=login>

12. *July 03, Associated Press* — **Small plane entered Camp David airspace.** A small plane violated the restricted airspace around the presidential retreat of Camp David, near Thurmont, north of Frederick, MD. The pilot was released late Saturday, July 2, without being charged, Secret Service spokesperson Jonathan Cherry said. The small Cessna was intercepted by two F-16 fighters about eight miles from Camp David about 10:45 p.m., (EDT) Saturday, Federal Aviation Administration spokesperson Holly Baker said. The plane was forced to land at Frederick Municipal Airport in Frederick, MD. On Wednesday, June 29, the White House briefly went to red alert when another small plane entered restricted airspace around Washington, DC. President Bush was hurried from his residence to a safer location and lawmakers were ordered to evacuate the Capitol. Two fighters intercepted the twin-engine, propeller-driven plane eight miles northeast of the Capitol and escorted it to Winchester, VA. Source: <http://www.cnn.com/2005/US/07/03/airspace.violated.ap/index.html>

13. *July 01, Associated Press* — **Suspicious package investigated at Texas airport.** Four airline ticket counters and other parts of Austin-Bergstrom International Airport in Austin, TX, were temporarily shut down and evacuated Friday morning, July 1, as police investigated a suspicious package, a spokesperson said. Ticket counters and curbside check-ins for American Airlines, America West, Continental, and United were closed, as was an upper-level road next to the airport terminal. Police later determined the package, which was found abandoned by a security employee about 8:15 a.m. (CDT) at a United curbside check-in, contained a homemade model airplane refueler, said airport spokesperson Leslie Schneiweiss. The package included a battery, battery pack, pump, and a container to hold fuel, she said. Once the contents of the package were identified, operations at the airport began returning to normal about noon, Schneiweiss said. Source: [http://www.usatoday.com/travel/news/2005-07-01-austin\\_x.htm](http://www.usatoday.com/travel/news/2005-07-01-austin_x.htm)

14. *July 01, Associated Press* — **US Airways files reorganization plan.** Creditors of bankrupt US Airways will receive either 10% of the money owed them or stock in the new airline under a reorganization plan filed Thursday, June 30, in bankruptcy court. US Airways, the nation's seventh-largest carrier, filed for bankruptcy protection in September, its second trip into Chapter 11 since 2002. The airline hopes to emerge from bankruptcy by year's end by being acquired by America West Holdings, the parent of Arizona-based America West Airlines. It also has attracted \$500 million in new investments by outside parties, including regional carrier Air Wisconsin. According to the plan of reorganization, unsecured creditors with claims of less than \$50,000 would receive 10% of their claim, up to \$5,000. The largest unsecured creditor is the federal Pension Benefit Guaranty Corp., which took over the airline's under funded pension plans. Source: [http://www.usatoday.com/travel/news/2005-07-01-usair-reorg\\_x.htm](http://www.usatoday.com/travel/news/2005-07-01-usair-reorg_x.htm)

[\[Return to top\]](#)

## **Postal and Shipping Sector**

Nothing to report.

[\[Return to top\]](#)

## **Agriculture Sector**

**15. *July 05, Reuters* — Japan bird flu outbreak contained.** A ban on shipments of chickens from an area of Japan where two cases of bird flu were found last week is likely to be lifted later this month because the disease is being contained, a local agriculture official said on Tuesday, July 5. "We will lift a limit on chicken shipments around July 27, unless we detect any new case of the disease," the official in Ibaraki prefecture said. The prefecture reported the first outbreak of avian influenza in Japan since last year. Since the "H5N2" strain of the bird flu virus was detected at a farm in Ibaraki on June 26, the government has restricted the movement of chickens in a three mile radius around the farm to prevent the disease from spreading. The same strain of the virus was confirmed Friday, July 1, at another chicken farm close to where the first case was found. The official said the local government had checked all the chicken farms within the restricted area and found that fowl on five farms might have contracted the disease. Birds on the other 12 farms tested negative for the disease. The government finished killing more than 38,000 birds Monday, July 4, and will cull an additional 90,000 chickens on the affected farms.

Source: <http://www.alertnet.org/thenews/newsdesk/T124475.htm>

**16. *July 05, Illinois Ag Connection* — Veterinarians play vital role in homeland security.** More than 170 veterinarians from throughout Illinois are members of the Illinois Veterinary Emergency Response Team (IVERT). All have received training to respond to animal disease outbreaks, including foreign animal diseases and potential bioterrorism. "IVERT was developed to function as a National Guard of veterinarians," says Larry Firkins, associate professor at the University of Illinois College of Veterinary Medicine and member of IVERT. If an emergency arises, the veterinarians in IVERT will be called upon to leave their everyday jobs to address the crisis. IVERT is a program overseen by the Illinois Department of Agriculture. Veterinarians are trained to recognize and treat diseases that affect food animals. Early diagnosis of a disease is the key to preventing catastrophic outbreaks. Through programs like IVERT, veterinarians learn how to identify symptoms and signs of unusual or foreign diseases. Local veterinarians who have close relationships with cattle, swine, and poultry farmers and visit farms regularly can help farmers identify outbreaks early — ideally delivering a lab-tested diagnosis within 24 hours of seeing a sick animal.

Source: <http://www.illinoisagconnection.com/story-state.cfm?Id=521&y r=2005>

**17. *July 05, North Dakota Ag Connection* — State livestock owners alerted to anthrax potential.** Recent heavy rains and flooding in much of North Dakota have created prime conditions for anthrax, say state animal health officials. "Livestock owners in areas where anthrax has been recorded in the past should consult their veterinarians about having their animals vaccinated,"

said Beth Carlson, deputy state veterinarian. "Producers should also report any sudden or unusual livestock deaths to their veterinarians or to the State Board of Animal Health." Anthrax is a bacterial disease generally contracted by livestock after consuming spores found in the soil. Source: <http://www.northdakotaagconnection.com/story-state.cfm?Id=429&yr=2005>

18. *July 05, Associated Press* — **Risk of disease outbreaks prompt technology change.** The risk of spreading disease by disposing of animal carcasses in landfills has led to the University of Minnesota to turn to a contraption that turns tons of animal tissue into a sterile slurry suitable for the public sewer. "Every infectious disease we have is a risk on the outside to other animals. ... We're trying to solve animal disease problems, not contribute to them," said Jim Collins, director of the university's veterinary diagnostic lab. So this spring the university began using a \$2.3 million tissue digester, which resembles a giant pressure cooker filled with Drano. Officials say the system is potent enough to kill even mad cow disease and its cousins. The animal research and veterinary operations at the university dispose of up to a million pounds of remains annually, some of them leftover from necropsies at the St. Paul veterinary labs. For years, the university had buried the remains, incinerated some of them, or sent them to rendering plants. The remains with the most potential for danger were shipped to a biohazard site in North Dakota. However, in the past few years North Dakota stopped taking deer after chronic wasting disease appeared in Minnesota, and rendering plants also stopped accepting the waste. Source: <http://www.grandforks.com/mld/grandforks/news/state/12057742.htm>

19. *July 03, Associated Press* — **Experts don't expect more cases of mad cow.** After the first discovery of mad cow in the U.S. in 2003, some 700 head of cattle were killed as a precaution. Fears were high that Washington state's cattle market would collapse. Federal government experts suggested the industry nationwide could lose \$15 billion and others speculated it would not be surprising if a couple dozen infected animals were found. A year and a half later, experts say they have better information about the brain-destroying illness. U.S. Department of Agriculture (USDA) officials announced last week that a 12-year-old beef cow from Texas tested positive for mad cow disease but they don't expect to find another case. Back in 2003, officials didn't know how prevalent mad cow disease was in the U.S., USDA spokesperson Jim Rogers said. "Now we've tested just under 400,000 animals and we've found one case," Rogers said. "Now we're very confident to say if it's here, it's an extremely low level." The case announced last week was the first documented one in U.S. born and raised livestock. The only other known case of the disease in the U.S. involved a dairy cow that had come from Canada. Source: <http://abcnews.go.com/US/wireStory?id=904519>

[[Return to top](#)]

## **Food Sector**

20. *July 05, Guardian (United Kingdom)* — **Salmonella warning over Spanish lettuce.** Spanish vegetables are being watered with untreated sewage in parts of Spain as farmers battle to raise crops in a severe drought. Spain's environment minister, Cristina Narbona, and Spanish newspapers raised the alarm after outbreaks of a resistant form of salmonella in Britain and Finland were linked to imported Spanish lettuce. Narbona warned cabinet ministers that more farmers in the vegetable-growing region of Murcia would use untreated sewage if clean



irrigation water were not made available. Farmers from Beniel, southeast Spain, yesterday told El País newspaper they were using untreated sewage. "The water we receive is not enough, so we are forced to mix it with the sewage from our own homes," a farmer said. Britain's Food Standards Agency confirmed Monday, July 4, that an outbreak of the resistant form of salmonella, Typhimurium DT104, in January had been linked to imported Spanish vegetables. The 96 reported cases were more than three times the norm for this kind of salmonella. Eleven people needed hospital treatment. "The source seemed to be iceberg lettuce from the Murcia region," a spokesperson said. Finland sent a warning around European Union after the same kind of salmonella struck people across western and southern parts of the country in May. Once again, the outbreak was traced back to iceberg lettuce imported from Spain.

Source: <http://www.guardian.co.uk/spain/article/0,2763,1521406,00,ht ml>

[[Return to top](#)]

## **Water Sector**

**21. *July 01, Arizona Republic* — Water treatment plants face audit.** An outside consultant will perform a comprehensive audit of each of Phoenix, AZ's five water treatment plants in the wake of a water scare at one of the facilities earlier this year. Members of a subcommittee charged with looking into the failures at the Val Vista Water Treatment Plant said that they wanted each of the plants evaluated after the consultant, Metcalf & Eddy, determined that bad decision making, and not mechanical failure, caused the water debacle in late January. Officials fear that because the problems were endemic to the department's operations, similar situations could arise at the city's other water treatment facilities. The January incident began after the Val Vista plant in Mesa, which co-owns the facility with Phoenix, began pumping cloudy, or turbid, water into Phoenix's pipelines. The water did not meet federal safe-drinking water standards. More than 1.5 million residents were told to boil water for two days. The consultant also will evaluate a new water treatment plant still under construction.

Source: <http://www.azcentral.com/news/articles/0701phx-water01.html>

[[Return to top](#)]

## **Public Health Sector**

**22. *July 05, BBC News* — Indonesia polio cases increase.** A further 21 cases of polio have been found in Indonesia, bringing the total to 100, the World Health Organization (WHO) said. Twenty of the new cases are in Banten, West Java, Indonesia, the location of the first case in the current outbreak. Another new case is on the island of Sumatra, which was polio-free until last week. Officials believe the outbreak can be traced to Nigeria, where vaccinations were suspended in 2003 after radical clerics said they were part of a U.S. plot. Tuesday, July 5's information brings the number of polio cases on Sumatra to two—the first was confirmed last week. They are of concern to the WHO because they suggest the disease has jumped islands. Indonesia first detected a case in the West Java province in April. Indonesian officials say the virus could have been picked up by a pilgrim on the hajj to Mecca, or a migrant worker. Polio is still endemic in six countries: Afghanistan, Egypt, India, Nigeria, Niger, and Pakistan. The United Nations has been campaigning to eradicate the disease by the end of this year.

Source: <http://news.bbc.co.uk/2/hi/asia-pacific/4651841.stm>

23. *July 05, Agence France-Presse* — **Global plan to halt bird flu unveiled, but millions needed in funds.** A global strategy to control the deadly bird flu virus within a decade was released by United Nations and animal health experts, who appealed for millions in donor funds to make the plan a reality. With the virus already detected in other regions such as Europe, major outbreaks anywhere in the world "can happen any time because of international trade and movements of animals, people and products," stated Joseph Domenech, chief veterinary officer for the UN's Food and Agriculture Organization (FAO). The global plan, written by the FAO and the World Organization for Animal Health in collaboration with the World Health Organization, calls for 102 million dollars to fight the disease in animals over the next three years. The global strategy calls for an initial focus on Southeast Asia, East Asia and South Asia, and for the measures to be rolled out to the rest of Asia as well as Africa, America, and Europe by October. Among the recommendations, it calls for more research into the H5N1 virus, and better surveillance of animals so that outbreaks of the disease can be detected and prevented as early as possible.

Source: [http://news.yahoo.com/news?tmpl=story&u=/afp/20050705/hl\\_afp/healthflumalaysia\\_050705071703](http://news.yahoo.com/news?tmpl=story&u=/afp/20050705/hl_afp/healthflumalaysia_050705071703)

24. *July 04, Kyodo News* — **World Health Organization warns deadly bird flu virus tightening its grip in Asia.** Confounded by the deadly bird flu virus, the World Health Organization (WHO) called for countries Monday, July 4, to prepare for the worst. Shigeru Omi, WHO regional director for the Western Pacific, stressed the danger caused by the H5N1 virus is not receding. "The virus has tightened its grip on the region...It has behaved in ways that suggest it remains as unstable, unpredictable and versatile as ever. Judging by its performance to date, we need to be on constant alert for surprises," he said in an opening speech at an international meeting on avian influenza in Kuala Lumpur. While scientists are still trying to figure out how the virus spreads to humans, they are mystified by the recent death of 6,000 migratory birds in China's Qinghai Province. "Wild birds have always been considered reasonably resistant to H5N1, so we see this worrying development as yet another example of how unpredictable the virus can be," Omi said. Experts from the WHO and other agencies from the United Nations are participating in a three-day meeting concerning the interaction between humans and the production, distribution, processing and marketing of animals for food, which has been identified as the root cause of the problem.

Source: <http://asia.news.yahoo.com/050704/kyodo/d8b4etf80.html>

25. *July 04, Canadian Broadcasting Corporation* — **Birds becoming immune to West Nile virus.** Birds seem to be developing the ability to fight off West Nile virus, reducing the likelihood that humans may contract the disease, scientists say. Studies conducted in eastern North America, where the virus first appeared on the continent, show birds are becoming immune to the virus. "This virus is maintained in a bird-mosquito life cycle," Margo Pybus, a wildlife disease expert with Canada's Alberta Fish and Wildlife, said. "So if you have increasing immunity in birds and mosquitoes...[there is] less virus to spill over into humans, when humans might get bitten by mosquitoes." Dr. Karen Grimsrud, Alberta, Canada's deputy health officer, said even if birds become immune to the virus, people still need to be cautious. Pybus said it's difficult to say how quickly birds become immune, and how much of the population will gain protection.

Source: <http://www.cbc.ca/stories/2005/07/04/West-Nile050704>

26. *July 03, Milwaukee Journal Sentinel (WI)* — **Mosquitoes infect each other with West Nile virus.** Scientists have discovered a new method by which the West Nile virus can pass from one host to another. Researchers at the University of Texas Medical Branch in Galveston have found that a mosquito can acquire the virus simply by feeding next to an infected mosquito, even if the host animal doesn't have virus in its bloodstream. Stephen Higgs, lead author of the study, studied the virus transmission by placing two coffee mug-sized cans side by side. One contained infected mosquitoes and the other uninfected mosquitoes. The cans were covered by a fine mesh screen, across which the team laid a sedated mouse. This allowed the mosquitoes to feed at the same time even though the two sets of mosquitoes could not physically interact. The experiment, repeated five times, consistently showed that two to six percent of the uninfected mosquitoes ultimately acquired the virus. Though the findings challenge conventional wisdom of how viruses can spread, scientists emphasize that the new route does not put humans at greater risk.

Source: <http://www.jsonline.com/alive/news/jul05/337993.asp>

[\[Return to top\]](#)

## **Government Sector**

Nothing to report.

[\[Return to top\]](#)

## **Emergency Services Sector**

27. *June 29, San Jose Mercury News (CA)* — **Hospitals assist in terror drill.** Two simulated early morning explosions at Caltrain stations in San Jose and Mountain View in Northern California release toxic nerve gas. Hospitals brace for the worst. For a few hours on Wednesday, June 29, nine Santa Clara County hospitals pretended this scenario was real. In a drill called "Operation Spray & Wash," coordinated by the county public health department, hospitals set up shower tents in their parking lots and scrubbed down volunteers posing as terror victims. Twenty-eight volunteers posed as patients at Regional, including Boy Scouts and staff members who came in on their day off. The 204-bed Regional Medical Center of San Jose went into lockdown, closing off many of its 33 doors and monitoring the remaining entrances "so contaminated people don't walk in willy-nilly," Benlice said. Regional spokesperson Victoria Emmons said the hospital also kept an eye on weather conditions, trying to guess which way the plumes of gas would spread and how this might affect the number of patients streaming in. Emmons said one of the goals was to test communication between the hospitals and the county's command center.

Source: [http://www.mercurynews.com/mld/mercurynews/news/breaking\\_news/12017121.htm](http://www.mercurynews.com/mld/mercurynews/news/breaking_news/12017121.htm)

[\[Return to top\]](#)

## **Information Technology and Telecommunications Sector**

28.

*July 04, FrSIRT* — **Sun Java Desktop System (JDS) applet security bypass vulnerability.** A vulnerability was identified in Sun Java Desktop System (JDS) for Linux, which could be exploited by malicious Websites to compromise a vulnerable system. This flaw is due to an unspecified error when handling specially crafted applets, which may be exploited, via a malicious Webpage, to bypass the default security policy and read/write arbitrary files on a vulnerable system or execute local applications with the privileges of the user running the untrusted applet. Users should upgrade to Sun Java Desktop System (JDS) Release 2 with the updated RPMs patch 118752-02.

Sun advisory 101799: [http://sunsolve.sun.com/search/document.do?assetkey=1-26-101\\_799-1](http://sunsolve.sun.com/search/document.do?assetkey=1-26-101_799-1)

Source: <http://www.frstirt.com/english/advisories/2005/0950>

29. *July 04, Secunia* — **phpGroupWare XML-RPC PHP code execution vulnerability.** A vulnerability has been reported in phpGroupWare, which can be exploited by malicious people to compromise a vulnerable system. Users should restrict access to scripts using the XML-RPC functionality.

Source: <http://secunia.com/advisories/15917/>

30. *July 04, Secunia* — **Cacti security bypass and shell command injection .** Two vulnerabilities have been reported in Cacti, which can be exploited by malicious people to bypass certain security restrictions and compromise a vulnerable system. 1) Input passed to the "[no http headers](#)" parameter isn't properly verified before being used. This can be exploited to overwrite session structures and bypass certain filtering mechanisms. Successful exploitation allows people to gain administrative privileges and perform various SQL injection attacks, but requires that "register\_globals" is enabled. 2) An error in the administrative interface can be exploited to inject arbitrary shell commands by manipulating the path to "rrdtool". Successful exploitation requires administrative privileges. The vulnerabilities have been reported in version 0.8.6e and prior.

Users should update to version 0.8.6f: [http://www.cacti.net/download\\_cacti.php](http://www.cacti.net/download_cacti.php)

Source: <http://secunia.com/advisories/15908/>

31. *July 01, zone-h* — **Phishing problems on MSN.** Multiple phishing problems exist on support.msn.com, permitting to a possible attacker to conduct phishing attack against a user. 1) Input passed to the "ru" parameter in "pplogin.aspx" isn't properly sanitized before being returned to the user. 2) Input passed to the 'mssplogin' parameter isn't properly sanitised, and by using specially crafted URL an attacker can cause the user to be redirected to an arbitrary URL for the passport authentication. Another phishing problem exists on login.passport.net. The problem is caused due to input passed to the "ru" in "uilogout.srf" isn't properly sanitised. By using specially crafted URL an attacker can cause the user to be redirected to an arbitrary URL for the passport authentication.

Source: <http://www.zone-h.org/advisories/read/id=7764>

## Internet Alert Dashboard

#### DHS/US-CERT Watch Synopsis

**Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.**

**US-CERT Operations Center Synopsis:** US-CERT reports a working public exploit for a vulnerability in the Microsoft JVIEW Profiler (javaprx.dll) component, an interface to the Microsoft Java Virtual Machine. This vulnerability can be exploited when a user attempts to view an HTML document (e.g., a web page or an HTML email message) that attempts to instantiate the JVIEW Profiler COM object in a certain way. Successful exploitation could allow an attacker to execute arbitrary code on the user's system with privileges of the user. More information about this vulnerability can be found in the following US-CERT Vulnerability Note: VU#939605: VIEW Profiler (javaprx.dll) COM object contains an unspecified vulnerability. Microsoft has published a Security Advisory about this issue and is continuing to investigate the problem. Until a patch is available to address this vulnerability, US-CERT strongly encourages users to review the workarounds section of Vulnerability Note VU#939605.

#### Current Port Attacks

<b>Top 10 Target Ports</b>	445 (microsoft-ds), 6881 (bittorrent), 27015 (halflife), 1433 (ms-sql-s), 1026 (----), 80 (www), 135 (epmap), 139 (netbios-ssn), 6346 (gnutella-svc), 8956 (----) Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center
----------------------------	--

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://www.us-cert.gov).

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

## **Commercial Facilities/Real Estate, Monument & Icons Sector**

Nothing to report.

[\[Return to top\]](#)

## **General Sector**

32. *July 04, Associated Press* — **Terror groups believed to be in Canada.** Though many view Canada as an unassuming neutral nation that has skirted terrorist attacks, it has suffered its share of aggression, and intelligence officials believe at least 50 terror groups now have some presence there. They are from Sri Lanka, Kurdistan, and points between and include supporters of some of the best-known Mideast groups, including al Qaeda, authorities say. Osama bin Laden named Canada one of five so-called Christian nations that should be targeted for acts of terror. The others, reaffirmed last year by his al Qaeda network, were the U.S., Britain, Spain, and Australia. The Canadian Security Intelligence Service (CSIS), counterpart of the CIA, said terrorist representatives are actively raising money, procuring weapons, "manipulating immigrant communities" and facilitating travel to and from the U.S. and other countries.



Besides al Qaeda, those groups include Islamic Jihad, Hezbollah and other Shiite groups, Hamas, the Palestinian Force 17, Egyptian Al Jihad, and various other Sunni groups from across the Middle East, CSIS said. The Irish Republican Army, Tamil Tigers, Kurdistan Workers Party (PKK), and major Sikh terrorist groups also have supporters in Canada.

Source: <http://sfgate.com/cgi-bin/article.cgi?f=/n/a/2005/07/04/international/i092329D03.DTL>

[\[Return to top\]](#)

## **DHS/IAIP Products & Contact Information**

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

[DHS/IAIP Daily Open Source Infrastructure Reports](#) – The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website:

<http://www.dhs.gov/iaipdailyreport>

[Homeland Security Advisories and Information Bulletins](#) – DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: <http://www.dhs.gov/dhspublic/display?theme=70>

### **DHS/IAIP Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS/IAIP Daily Report Team at (703) 983-3644.

Subscription and Distribution Information:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS/IAIP Daily Report Team at (703) 983-3644 for more information.

### **Contact DHS/IAIP**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **DHS/IAIP Disclaimer**

The DHS/IAIP Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.